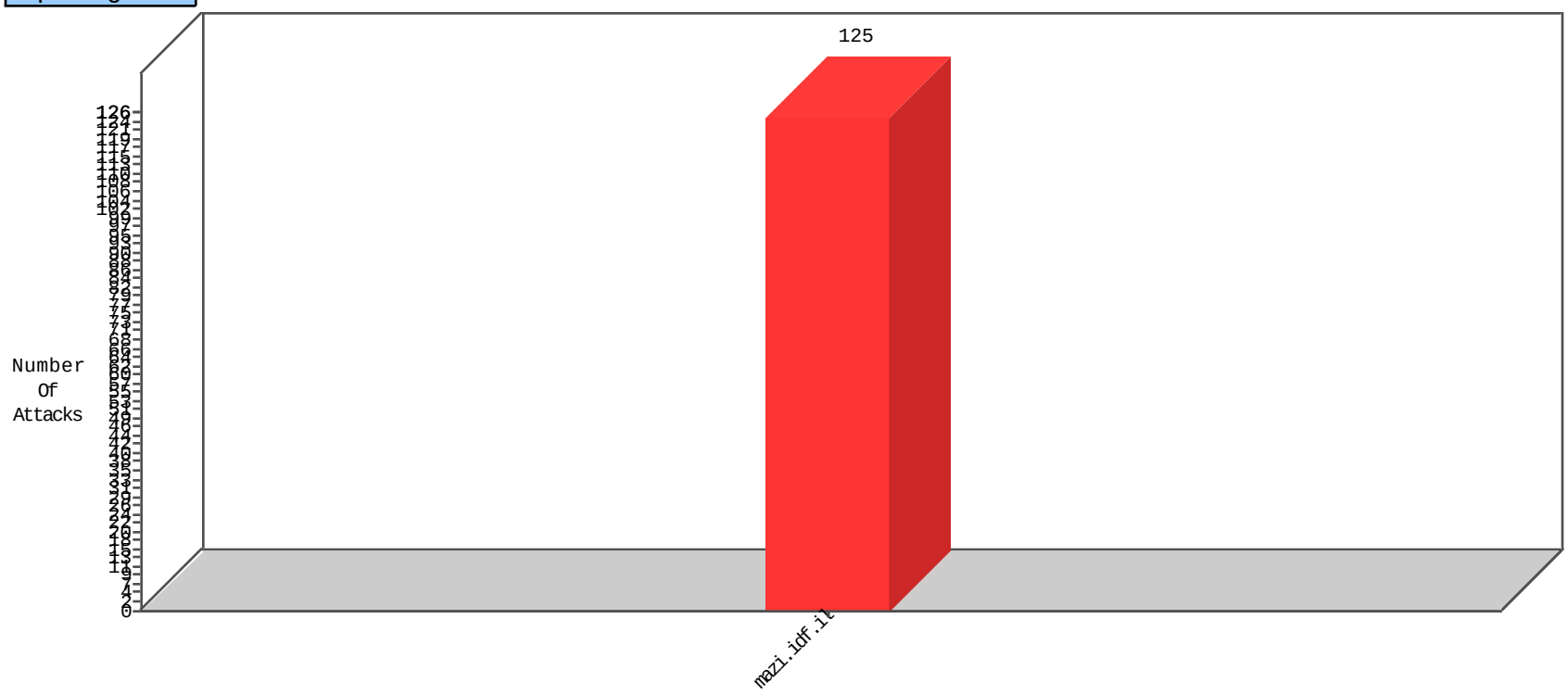
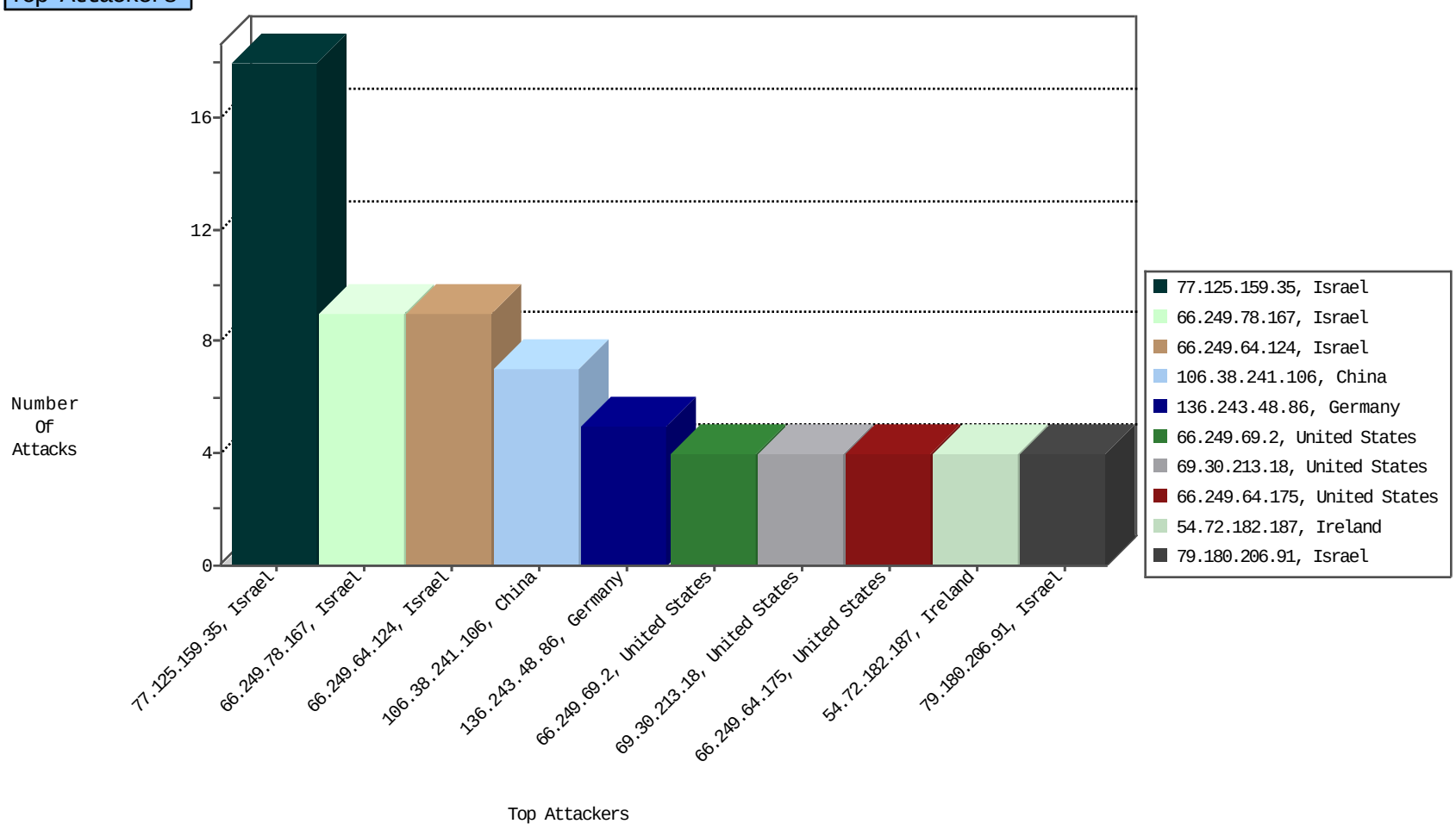
02-25-2016 to 02-26-2016

Focused IP Under Attack Daily Report

Top Targets



Top Attackers



02-25-2016 to 02-26-2016

Top Attackers In DDoS-Defence

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	DP_location.Location	Count
54.72.182.187	Ireland	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	NetV-London	4
79.180.206.91	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	3
136.243.48.86	Germany	147.237.77.17	mazi.idf.il	JLM_Purple_Con_Limit_Http	drop	NetV-London	3
82.81.37.46	Israel	147.237.77.17	mazi.idf.il	Block_Udp_All_Nets	drop	BBL-Israel	2
136.243.48.86	Germany	147.237.77.17	mazi.idf.il	JLM_Under_Attack_Con_Http	drop	NetV-London	2
184.105.139.76	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
184.105.139.98	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1
198.23.190.39	United States	147.237.77.17	mazi.idf.il	Block_Ntp_All_Net	drop	NetV-London	1

02-25-2016 to 02-26-2016

Top Attackers In IPS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
77.125.159.35	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
66.249.78.167	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
66.249.64.124	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
106.38.241.106	China	147.237.77.17	mazi.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
69.30.213.18	United States	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	4
66.249.64.2	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
66.249.75.18	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.9.131.69	Germany	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
2.54.128.221	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.64.8	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
10.0.0.9		147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.162.167	United Kingdom	147.237.77.17	mazi.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.78.181	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.75.34	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
188.165.15.87	France	147.237.77.17	mazi.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.78.174	Israel	147.237.77.17	mazi.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-25-2016 to 02-26-2016

Top Attackers In IDS

Attacker Address	Attacker Geo	Target Address	Site	Signature	Count
93.174.93.144	Netherlands	147.237.77.17	mazi.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	United States	147.237.77.17	mazi.idf.il	ET DROP Dshield Block Listed Source	1

02-25-2016 to 02-26-2016

Top Attackers In FW

Attacker Address	Attacker Geo	Target Address	Site	Name	Signature	Device Action	Count
212.76.127.10	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	45
31.168.150.133	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
201.131.148.28	Panama	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
84.94.205.233	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.86.50	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.22	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	16
46.19.85.22	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
213.57.164.147	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
37.26.148.142	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
106.38.241.106	China	147.237.77.17	mazi.idf.i	drop	SAM rule	drop	15
195.160.242.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
195.239.16.40	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.76.127.111	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
109.66.210.200	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
195.239.16.53	Russian Federation	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.76.127.219	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.76.127.44	Israel	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
5.102.195.35	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.176	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
87.69.165.104	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
203.133.169.220	Korea, Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
80.179.9.7	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.176	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
87.69.165.104	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.81.99	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
195.160.242.40	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
84.109.36.217	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
85.65.81.99	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.135.181	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
203.133.169.220	Korea, Republic of	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	4
157.55.39.147	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.1.50	Israel	147.237.77.17	mazi.idf.i	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
157.55.39.162	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.113.91	United States	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
37.26.148.142	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
5.39.93.143	France	147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
84.94.32.197	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
185.89.217.233		147.237.77.17	mazi.idf.i	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
64.125.239.47	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
176.13.9.154	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
213.57.192.167	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	alert	1
89.248.174.4	Netherlands	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.109.160.210	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.105.134.220	Sweden	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.3.147.22	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
46.120.36.24	Israel	147.237.77.17	mazi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.39.227	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
213.57.164.147	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
208.115.113.91	United States	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.26.149.195	Israel	147.237.77.17	mazi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

02-25-2016 to 02-26-2016

Top Attackers In WAF

Attacker Address	Attacker Geo	Target Address	Site	Signature	Device Action	Count
85.65.81.99	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3849-5035-he/igf.aspx	Block	1
66.249.78.254	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.69.10	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4150-he/igf.aspx	Block	1
157.55.39.180	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/425-he/igf.aspx	Block	1
104.131.147.112	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
80.246.133.248	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/sip_storage/files/1/1351.jpg	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/55-he/igf.aspx	Block	1
185.3.147.37	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
66.249.69.2	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3433-he/igf.aspx	Block	1
65.55.218.54	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on mazi.idf.il/templates/newslist/undefined	Block	1
157.55.39.162	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/113-11581-he/ללא גבולות.aspx	Block	1
89.38.148.64	Romania	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4419-he/mailto:igf@idf.gov.il	Block	1
68.180.228.160	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/general/ה	Block	1
66.249.69.10	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/607-he/igf.aspx	Block	1
157.55.39.181	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6321-he/igf.aspx	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/robots.txt	Block	1
141.255.44.84	Greece	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templatecontrols/	Block	1
84.108.148.199	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/96-he/igf.aspx	Block	1
66.249.69.2	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/647-he/igf.aspx	Block	1
157.55.39.178	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/6578-9974-he/igf.aspx	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Multiple Unauthorized URL Access from 66.249.64.175	Block	1
89.138.89.160	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4944-he/igf.aspx	Block	1
77.125.9.161	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/newslist/undefined	Block	1
66.249.78.167	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/templates/shared/usercontrols/vodchannel/	Block	1
173.234.162.74	United States	147.237.77.17	mazi.idf.i	Parameter Type Violation catid in mazi.idf.il/templates/homepage/joinmailinglist.aspx	Block	1
66.249.64.180	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4278-he/igf.aspx	Block	1
157.55.39.147	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/4316-he/	Block	1
84.109.160.210	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/images/transvideocounter.gif	Block	1
66.249.78.248	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/5477-he/igf.aspx	Block	1
66.249.69.2	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/700-he/igf.aspx	Block	1
157.55.39.179	United States	147.237.77.17	mazi.idf.i	Distributed Unauthorized URL Access on 147.237.77.17/robots.txt	Block	1
66.249.64.175	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/4150-he/igf.aspx	Block	1
94.230.88.211	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage/files/7/6117.not	Block	1
79.180.206.91	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/3850-5216-he/igf.aspx	Block	1
66.249.78.242	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/113-he/igf.aspx	Block	1
176.13.20.18	Israel	147.237.77.17	mazi.idf.i	Unauthorized URL Access to mazi.idf.il/sip_storage	Block	1
66.249.69.2	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to 147.237.77.17/14-he/igf.aspx	Block	1
157.55.39.147	United States	147.237.77.17	mazi.idf.i	Unauthorized URL Access to www.mazi.idf.il/14-8347-he	Block	1

02-25-2016 to 02-26-2016